



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/518,664	03/03/2000	Cameron Mashayekhi	112024-0054	6178

21186 7590 09/11/2003

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER

ZIA, MOSSADEQ

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 09/11/2003

7

Please find below and/or attached an Office communication concerning this application or proceeding.

4

Office Action Summary

Application No.

09/518,664

Applicant(s)

MASHAYEKHI, CAMERON

Examiner

Mossadeq Zia

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03/03/2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 6.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Office Action Summary

Application No.

09/518,664

Applicant(s)

MASHAYEKHI, CAMERON

Examiner

Mossadeq Zia

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03/03/2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 6.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No.

5,818,936 Mashayekhi et al in view of Patent No. 5,784,566, Viavant et al.

3. In regards to claim 1, Mashayekhi et al, discloses an authentication system suitable for automatically providing authentication to a user at a client node, the user providing a user secret and requesting access to network resources resident at one or more server nodes in a distributed network system, said authentication system comprising (Mashayekhi, col. 3, line 25-28):

a local application program interface for receiving the user secret, said local application program interface in communication with a requested network resource (Mashayekhi, col. 5, line 38-44);

a cryptography service node (Key Generator and exchange controller) (Mashayekhi, fig. 2, label 207, 222) including means for providing a common key (private key) and algorithm (Mashayekhi, col. 5, 44-46, col. 8, line 7-8), and means for providing a client/server session key or "secure transfer" and algorithm (Mashayekhi, col. 5, line 61-63, col. 7, line 32-33, col. 8, line 8-10); and

an authentication database in communication with said local application program interface(fig.2, label 210, 240) and with said cryptography service node (Mashayekhi, fig. 2, label 222), said authentication database (Mashayekhi, fig. 2, label 204) including

an authentication secret (application secret) associated with the user (Mashayekhi, col. 5, line 62-63); means for encrypting said authentication secret using said common key (private key) and algorithm (Mashayekhi, col. 6, line 43, 45-47, 54-59).

Mashayekhi et al, shows that the common keys are transferred securely between client/server nodes (Mashayekhi, col. 8, line 7-9, fig. 2, label 207), but fails to show the means to encrypt the common key using the client/server session key and algorithm. However, Viavant, et al, teaches that encryption is a type of security service by which communication over a network are encoded to help ensure privacy of sensitive data (common key) (Viavant, col. 1, line 38-40, fig. 11), and that the encryption key (session key, fig. 12, label 234) should only be known to the sender and receiver (client/server) (Viavant, col. 1, line 42-43), where algorithms such as stream cipher RC4, developed by RSA Data security, Inc., is widely used as a method for high speed encryption (Viavant, col. 1, line 45-46) to encrypt network data. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Mashayekhi as per teaching of Viavant to include the benefit of high speed encryption in a networked computer environment because the transport of a encrypted common key during a client/server session (fig. 6) provides good security with relatively low total performance degradation (Viavant, col. 1, line 47-48).

4. In regards to claim 2, Mashayekhi et al and Viavant et al teach claim 1 as mentioned above, in addition teaches means for encrypting and decrypting said authentication secret using a secret store key and algorithm (Mashayekhi, col. 5, line 3-4, col. 6, line 58-59).

Art Unit: 2134

5. In regards to claim 3, Mashayekhi et al and Viavant et al teach claim 1 as mentioned above, in addition teaches a network resource identifier or “application program identifier” (Mashayekhi, col. 6, line 29, 40-42) associated with said requested network resource or “application object” (Mashayekhi, col. 6, line 26-27); and a network policy associated with the user (col. 6, line 28) and with said network resource identifier.

6. In regards to claim 4, Mashayekhi et al and Viavant et al teach claim 1 as mentioned above, in addition discloses authentication database further comprises a second network resource identifier associated with a second network resource (Mashayekhi, fig. 3, label 306b); a second authentication secret associated with the user (Mashayekhi, fig. 3, label 304b); and a second network policy associated with the user (Mashayekhi, col. 6, line 28, fig. 3, label 306b) and with said second network resource identifier.

7. In regards to claim 5, Mashayekhi et al and Viavant et al teach claim 4 as mentioned above, in addition discloses an authentication database further comprises means for encrypting and decrypting (Mashayekhi, col. 6, line 58) said second authentication secret (Mashayekhi, col. 5, line 63) using said secret store key and algorithm (Mashayekhi, col. 6, line 7).

8. In regards to claim 6, Mashayekhi et al and Viavant et al teach claim 4 as mentioned above, in addition discloses an authentication database further comprises means for encrypting and decrypting said second authentication secret using a second secret store key and algorithm (Mashayekhi, col. 5, line 37, col. 7, line 4-7).

9. In regards to claim 7, Mashayekhi et al and Viavant et al teach claim 1 as mentioned above, in addition discloses cryptography service further comprises means for generating an authentication secret from the user secret (Mashayekhi, col. 5, line 40-45).

Art Unit: 2134

10. In regards to claim 8, Mashayekhi et al and Viavant et al teach claim 1 as mentioned above, in addition discloses common key comprises a symmetric key (Mashayekhi, col. 8, line 8-10 and Viavant, fig 3. 132, 136, 140).

11. In regards to independent claim 9, Mashayekhi et al and Viavant et al teach claim 1 as mentioned above, in addition discloses a method for automatically authenticating a user at a network client node in a distributed network system in response to a user request for access to network resources resident in one or more server nodes, said authentication method comprising the steps of:

providing a network resource identifier (Mashayekhi, col. 6, line 29, 40-42), a network resource policy (Mashayekhi, col. 6, line 28), and an authentication secret to an authentication database (Mashayekhi, fig. 2, label 202), said network resource identifier associated with the requested network resource (Mashayekhi, col. 6, line 26-27); retrieving said authentication secret in response to said user request (Mashayekhi, fig. 4a), said authentication secret associated with the user (Mashayekhi, col. 5, line 18-21) and with said network resource identifier (Mashayekhi, fig. 4a, block 410); encrypting said authentication secret with a common key and algorithm (Mashayekhi, col. 6, line 54-59); encrypting said common key and algorithm with a client/server session key and algorithm (encoded) (Mashayekhi, col. 7, line 32-33, col. 8, line 7-9, fig. 2, label 207, and see Viavant teaching in claim 1); and providing said encrypted authentication secret (encrypted data) and said encrypted common key (private key) to the client node (Mashayekhi, col. 7, line 36-37, 44-47).

Art Unit: 2134

12. In regards to claim 10, Mashayekhi et al and Viavant et al teach claim 9 as mentioned above, in addition discloses the steps of decrypting said encrypted common key using said client/server session key (Mashayekhi, col. 8, line 7-9); decrypting said encrypted authentication secret using said decrypted common key and algorithm (Mashayekhi, fig. 4b); and providing said decrypted authentication secret to the requested network resource (Mashayekhi, fig. 4b, block 424).

13. In regards to claim 11, Mashayekhi et al and Viavant et al teach claim 9 as mentioned above, in addition discloses the step of accessing said network resource policy prior to said step of retrieving said authentication secret, said network resource policy associated with the user and with said network resource identifier (Mashayekhi, col. 5, line 14-17).

14. In regards to claim 12, Mashayekhi et al and Viavant et al teach claim 9 as mentioned above, in addition discloses obtaining a list of client algorithms supported by the client node (Viavant, fig. 5, label 166); obtaining a list of server algorithms supported by the server node (fig. 5, label 168); comparing said list of client algorithms with said list of server algorithms so as to determine the strongest algorithm common to both said list of client algorithms and said list of server algorithms (Viavant, fig. 5, label 168); and using said strongest algorithm as said common key and algorithm.

15. In regards to claim 13, Mashayekhi et al and Viavant et al teach claim 9 as mentioned above, in addition discloses that the common key comprises a symmetric key (Mashayekhi, col. 8, line 8-10).

16. In regards claim 14, Mashayekhi et al and Viavant et al teach claim 9 as mentioned above, in addition discloses negotiating the strongest common algorithm between server and

Art Unit: 2134

client node (Viavant, fig. 5); and using said strongest algorithm as said client/server session key and algorithm (Viavant, fig. 9).

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is (703)305-8425. The examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (703)308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-3900.

Mossadeq Zia
Examiner
Art Unit 2134

mz
8/22/03

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134